FortiNAC

Mist
Wireless Integration

Version: 9.4

Date: April 21, 2025

Rev: H

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

Contents

Overview

The information in this document provides guidance for configuring the Mist wireless Access Point to be managed by FortiNAC. This document details the items that must be configured.

Note: As much information as possible about the integration of this device with FortiNAC is provided. However, the hardware vendor may have made modifications to the device's firmware that invalidate portions of this document. If having problems configuring the device, contact the vendor for additional support.

What it Does

FortiNAC provides network visibility (where endpoints connect) and manages network access for wireless endpoints connecting to Access Points. FortiNAC supports individual SSID configuration and management for this device.

How it Works

Visibility

FortiNAC learns where endpoints are connected on the network using the following methods:

- RADIUS communication
- L2 Polling (MAC address table read)
- L3 Polling (ARP cache read)

Control

FortiNAC provisions an endpoint's network access by managing VLAN assignments based on the Mist's model configuration or an applicable network access policy and the host state of the device. The VLAN configuration is modified using the appropriate method based upon the vendor and model (see chart below).

Device Support Methods

Endpoint Connectivity Notification	Reading MAC Address Tables (L2 Poll)	Reading IP Tables (L3 Poll)	Reading VLANs	VLAN Assignment	Reading SSIDs	De-auth
RADIUS (802.1x or MAC-auth)	API*	API*	API*	RADIUS**	API*	RADIUS** Disconnect (UDP 3799)

*API communication is between FortiNAC and Mist cloud controller. See Requirements for supported domains.
**RADIUS communication is between FortiNAC and Mist Access Point.

RADIUS Authentication

- FortiNAC learns of endpoints connecting from the Mist using RADIUS Authentication (When an endpoint disconnects, the status will change to “offline” upon the next L2 poll.

  When a wireless client attempts to connect, the Mist sends a RADIUS request to FortiNAC.

- **MAC-based Authentication**: Endpoints are authenticated based on the MAC address. This requires no configuration on the endpoint.

- **802.1x Authentication**: Endpoints are authenticated based on user information. This requires supplicant configuration on the endpoint and an authentication server (either FortiNAC local RADIUS server or a third party server).

Requirements

FortiNAC
Minimum FortiNAC software version:

- 8.8 and greater (using API domain api.mist.com)
- 9.4.2 and greater (using any Mist API domain)

Mist

- Supported Firmware Version: 0.5.17360 or greater
- Account for API access (full permissions)
- Supported API domains:
  - FortiNAC Software Engine Version 9.4.1 and lower: api.mist.com
  - FortiNAC Software Engine Version 9.4.2 and greater: Any Mist API domain
- Disable Fast-roaming (currently unsupported)

Considerations

- Mist is currently limited to 5000 API calls per hour. Care should be taken when determining the L2 poll frequency. For details, see Enable Enforcement.

Step 1: Confirm Network Access is Working

Before integrating with FortiNAC, set up the Mist on the network and ensure that it is working correctly:

- Consider creating a SSID for testing purposes.
- Take into account all VLANs needed for Production and Isolation.
- Confirm hosts can connect to the device and access the network. If 802.1x is used with a 3rd party RADIUS server, ensure authentication completes as expected.

When the device is running on your network, then begin the integration process with FortiNAC.

Step 2: Configure Mist

General Configuration Notes

- **Avoid certain characters:** When configuring the device itself, use only letters, numbers and hyphens (-) in names for items within the device configuration, in SNMP and CLI credentials. Other characters may prevent FortiNAC from reading the device configuration. For example, in many cases the # sign is interpreted by FortiNAC as a prompt. Cisco restricts the use of @ and #.
- **Network devices should have static IP addresses (or dynamic IP addresses that are reserved)**. Once a device that provides network services had been identified in FortiNAC there is no mechanism to automatically update the IP address for that device if there is a change. If the IP address on the device itself is changed, the device appears in FortiNAC to be offline or to have a communication error.

1. Record the Mist Site ID. This will be used when adding the device to FortiNAC.

   The Site ID can be retrieved from the Monitor page, or other https://manage.mist.com pages. Site ID is in the form of " xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "

   Example:

https://manage.mist.com/admin/?org_id=ORG_ID#!dashboard/insights/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

   Alternatively, use Mist API. Navigate to the following URL

   https://<*API domain*>/api/v1/self

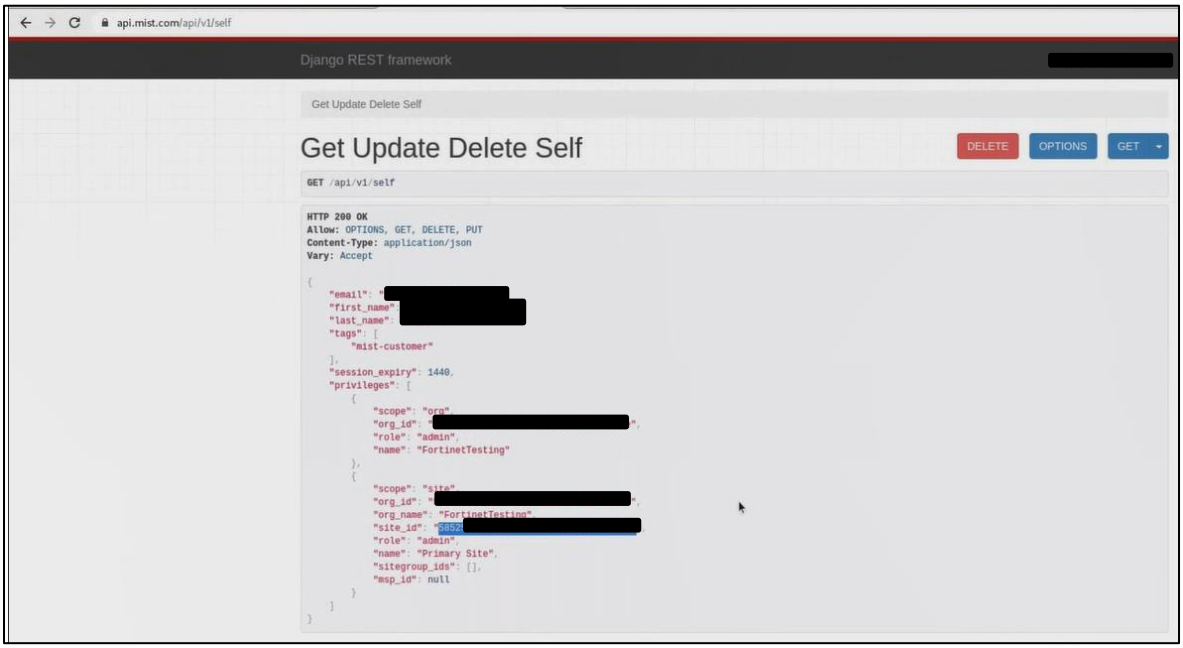
   Examples

   https://api.mist.com/api/v1/self

   https://api.ac2.mist.com/api/v1/self

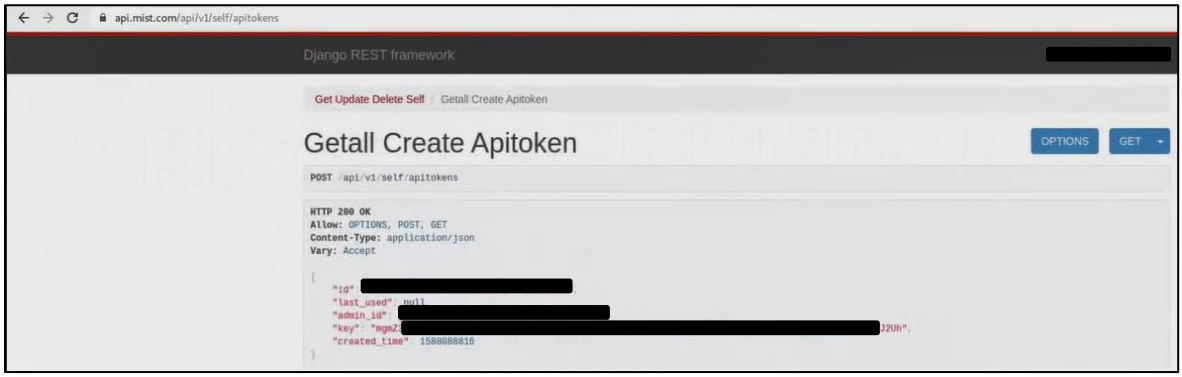
   https://api.eu.mist.com/api/v1/self

Record the value for “site_id”:



2. Generate API key.
    a. Using Mist API go to

       https://<*API domain*>/api/v1/self/apitokens
    b. Click **POST** to generate key.
    c. Refresh page.
    d. Once key is displayed, copy and paste to a text file immediately. **Note:** Key is only viewable once.



3. Configure RADIUS Authentication on each WLAN/SSID to be managed by FortiNAC.
    a. Navigate to https://manage.mist.com/admin/?org_id=<YOUR_ORG_ID>#!wlan/<YOUR_SITE_ID>
    b. Click **Network > WLANs**.
    c. Edit the existing WLANs or create new ones for FortiNAC to manage. The values in the table below are required when integrating with FortiNAC. Configure all other settings as appropriate. Refer to vendor documentation for additional information.

RADIUS Authentication Servers	**IP Address**: FortiNAC Server/Control Server eth0 IP Address **Port**: 1812 **Password/Shared Secret**: The RADIUS Secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration. **High Availability (HA) Environments**: Click **ADD AUTH SERVER** and add Secondary Server information (Do not use Shared IP Address).
RADIUS Accounting Servers	**IP Address**: FortiNAC Server/Control Server eth0 IP Address **Port**: 1813 **Password/Shared Secret**: The RADIUS Secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration. **High Availability (HA) Environments**: Click **ADD ACCOUNTING SERVER** and add Secondary Server information (Do not use Shared IP Address).
NAS IP Address	Access Point IP Address or left blank
CoA/DM Server	**Enabled** **IP Address**: FortiNAC Server/Control Server eth0 IP Address **Password/Shared Secret**: The RADIUS Secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration. **Local Port**: 3799 **Event-Timestamp:** Optional (FortiNAC does not include the Event-Timestamp attribute in CoA messages. Therefore, if this is set to "Mandatory", the CoA packets would be discarded). Click the “?” for more information. **High Availability (HA) Environments**: Click **ADD ACCOUNTING SERVER** and add Secondary Server information (Do not use Shared IP Address).

VLAN	Select **Dynamic** **Static:** VLAN assigned when no dynamic VLAN is applied (default) **VLAN Type: Standard(Tunnel-Private-Group-ID)** **Dynamic VLAN ID**: Add each VLAN that could potentially be assigned by FortiNAC

Step 3: Configure RADIUS in FortiNAC

Configure the appropriate RADIUS server option.

- Proxy
  - Authentication: FortiNAC processes RADIUS MAC but proxies 802.1x EAP authentication to a customer-owned (external) RADIUS server.
  - Accounting: FortiNAC proxies accounting traffic to a customer-owned (external) RADIUS server.
  - For more information on this option, see Proxy in the Administration Guide.
- Local
  - Authentication: FortiNAC's Local RADIUS Server processes RADIUS MAC and 802.1x EAP authentication without the need to proxy to an external RADIUS server.
  - Accounting: The Local RADIUS server does not provide accounting. If accounting is required, FortiNAC can be configured to proxy Accounting traffic to an external RADIUS server.
  - For more information on this option, see Local RADIUS Server in the Administration Guide.

These modes can be configured in FortiNAC on a per-device basis.

Step 4: Model the Device

For the FortiNAC software to recognize the device, it must be added to Inventory either by prompting the FortiNAC software to discover the device or by adding it manually. Regardless of how the device is added, the FortiNAC software must be able to communicate with it.

1. Login to the FortiNAC CLI as root.
2. Run the API tool to add the Mist device to the FortiNAC database. Use the API key and site ID recorded in previous section.

CloudAPITool -domain *<API_DOMAIN>* -action discovery -port 443 -apikey "*<API_KEY>*" -site *<SITE_ID>* -container *<container>*

Note:

- If container is specified but does not exist, it will be created.
- If no container is specified, the AP's will be added to a container named "MistWirelessAPs".

Step 5: Configure Logical Networks

Logical Networks are created in order to represent a specific level of network access. See section Logical networks of the Administration Guide for an overview of how they work. See Configuring logical networks for instructions.

Step 6: Develop Policies for Network Access (Optional)

Create Network Access Policies for dynamically provisioning network access for registered hosts when they connect to the network. Network Access Policies are very helpful when the VLAN assigned for unrestricted access can change depending upon the type of device connecting. See section Network access in the Administration Guide for an overview of how they work.

1. Build the components:

   Network Access Configuration: Assigns the appropriate network access value. See section Add or modify a configuration of the Administration Guide for details.

   User/Host Profile: Defines the criteria that will be used for hosts to match the policy. See section User/host profiles of the Administration Guide for more information.
2. Create the Network Access policy using the User/Host Profile and Network Access Configuration. For details, see Add or modify a policy of the Administration Guide.
3. Adjust ranking as appropriate. Starting with rank 1, user and host data is compared to each policy until a match is found.

Step 7: Review Enforcement Checklist

Before enabling enforcement, verify the following:

- There are no rogue MAC addresses connected to the SSID.

  Important: Rogue MAC addresses detected on enforced ports will be isolated.
- Isolation VLANS are working. Test client in isolation VLAN is able to:
  - Obtain IP address via DHCP (if scopes are defined in ConfigWizard)
  - Access the Portal (if configured)

Step 8: Enable Enforcement

To place SSIDs under FortiNAC's control, assign VLANs and enable enforcement for the various host states. This can be done in two ways

- Per Device Model – Applies to all SSIDs belonging to that model, unless there is a custom configuration applied to the SSID.
- Per SSID – Applies to the specific SSID. Can use configuration set in the model as well as custom configurations specific to the SSID.

Important:

- Always validate behavior on a test SSID first.
- The RADIUS Secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration.

1. Under **Network > Inventory** select the device model and click **Model Configuration.**
2. Fill in the fields as appropriate for the below sections.

RADIUS Mode	Proxy (default)
RADIUS Primary Server	Applies to 802.1x authentication only: Either the default RADIUS server or a pre-configured RADIUS server must be selected. RADIUS servers are configured on the RADIUS Settings window.
RADIUS Secondary Server	Applies to 802.1x authentication only: Either the default RADIUS server or a pre-configured RADIUS server must be selected. RADIUS servers are configured on the RADIUS Settings window.
RADIUS Shared Secret	Required for both MAC and 802.1x authentication. Must match the value entered on the device itself and the value entered on the RADIUS settings window.

3. Click the **Read VLANs** button. This populates the drop-down lists for the different connection states, such as Registration. Data in the drop-down lists represents the VLANs created on the device.
4. Select a setting in **Access Enforcement** for each host state.
5. In the **Access Value** column select a VLAN for each host state desired to enforce.
6. In the **Preferred Container** field, select the Container in Topology which the Wireless Access Points should be placed as they are discovered.
7. Click **Save**.
8. Click **Polling** tab.

9. Enter the appropriate L2 (Hosts) Polling value (minutes) based on the chart below. For best performance, it is recommended not to go lower than the specified value.

   Example:

   Total number of Access Points modeled in Topology: 800

   Acceptable values: 15, 20, 30, 60

   Not recommended: 10, 5

Total Number of Access Points	Recommended Lowest Value
700 and below	10 minutes
800	15 minutes
1000	20 minutes
2000	30 minutes
2500	60 minutes

Step 9: Validate

1. Connect a rogue host to the newly enforced SSID.
2. Verify the following:
   - Host is moved to the isolation VLAN
   - Host is able to access the captive portal (if configured)
   - Register the system and make sure it gets moved to the appropriate VLAN.

If any of the above do not work as expected, refer to the Troubleshooting section of this document.

Update FortiNAC After Controller or AP Changes

For proper functionality, FortiNAC should be updated when any of the following components are changed or added to the controller:

- APs
- SSIDs
- VLANs
- AP's IP Address

If this is not done, FortiNAC will not be able to be configured to use these components in the Device Model.

This update is done using the **Resync Interfaces** tool in the UI. There are two ways to run the tool:

- **Manual Update**: See Resync Interfaces in the Administration Guide for instructions.
- **Automated Update using Scheduler**: See section Add a task in the Administration Guide for instructions.
  - From the list of system actions, select **Resynchronize Device**.
  - From the **Group** dropdown list, select the group on which the action will be performed. The list contains only the group types specific to that Action. The WLCs are automatically part of the **L2 Wireless Devices** group. If desired, a new device group could be created.
  - From the **Schedule Type** drop down list, select either Fixed Day or Repetitive and set the day and time that the task is to be performed. It is suggested to run the task daily.

Troubleshooting

Related KB Articles

Refer to the applicable KB article(s):
Troubleshooting API errors in Mist integrations
Troubleshooting SNMP Communication Issues.
Troubleshooting Poll Failures
Online wireless hosts displaying offline status
Rogue Wireless Clients Cannot Connect to SSID
Troubleshooting RADIUS clients not connecting
Troubleshooting Wireless Clients Moved to the Wrong VLAN

Debugging

Use the following KB article to gather the appropriate logs using the debugs below.
Gather logs for debugging and troubleshooting

Note: Debugs disable automatically upon restart of FortiNAC control and management processes.

Function	Syntax	Log File
FortiNAC Server (Proxy RADIUS)	`nacdebug -name RadiusManager true`	/bsc/logs/output.master
FortiNAC Server (Local RADIUS)*	`nacdebug -name RadiusAccess true`	/bsc/logs/output.master
RADIUS Service (Local RADIUS)	`radiusd -X -l /var/log/radius/radius.log` Stop logging: Ctrl-C	/var/log/radius/radius.log
L2 related activity	`nacdebug -name BridgeManager true`	/bsc/logs/output.master
Vendor specific debugging	`nacdebug -name MistAP true`	/bsc/logs/output.master
Disable debug	`nacdebug -name <debug name> false`	N/A

*Logging for a given MAC Address:

```
nacdebug -logger 'yams.RadiusAccess.RadiusAccessEngine.00:11:22:33:44:55' -level FINEST
```

Disable:

```
nacdebug -logger 'yams.RadiusAccess.RadiusAccessEngine.00:11:22:33:44:55'
```

Other Tools

Send a RADIUS Disconnect (WLC C9800 only):

```
SendCoA -ip <devip> -mac <clientmac> -dis
```

Example:

```
SendCoA -ip 10.1.0.25 -mac 00:1B:77:11:CE:2F -dis
```